BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

PCT ORGANISATION MONDIALE DE LA PROPRIETE INTELLECTUELLE
Bureau international

DEMANDE INTERNATIONALE PUBLIEE EN VERTU DU TRAITE DE COOPERATION EN MATIERE DE BREVETS (PCT)

(51) Classification internationale des brevets 6 : G07F 7/10

A1

(11) Numéro de publication internationale: WO 99/06970

(43) Date de publication internationale: 11 février 1999 (11.02.99)

(21) Numéro de la demande internationale: PCT/FR98/01659

(22) Date de dépôt international: 27 juillet 1998 (27.07.98)

(30) Données relatives à la priorité:
97/09821 31 juillet 1997 (31.07.97) FR

(71) Déposant *(pour tous les Etats désignés sauf US)*: GEMPLUS S.C.A. [FR/FR]; Parc d'Activités de Gémenos, Avenue du Pic de Bertagne, F–13881 Gémenos Cedex (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(US seulement)*: SAPHAR, Louis–Pierre [FR/FR]; La Prairie, Bâtiment A2, 881, avenue Joseph Gasquet, F–83100 Toulon (FR). KARLISCH, Thierry [FR/FR]; Résidence Clair Soleil, F–13400 Aubagne (FR).

(74) Mandataire: NONNENMACHER, Bernard; Gemplus, Parc d'activités de Gémenos, Avenue du Pic de Bertagne, F–13881 Gémenos Cedex (FR).

(81) Etats désignés: AL, AU, BA, BB, BG, BR, CA, CN, CU, CZ, EE, GE, HU, ID, IL, IS, JP, KP, KR, LC, LK, LR, LT, LV, MG, MK, MN, MX, NZ, PL, RO, SG, SI, SK, SL, TR, TT, UA, US, UZ, VN, YU, brevet ARIPO (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Publiée

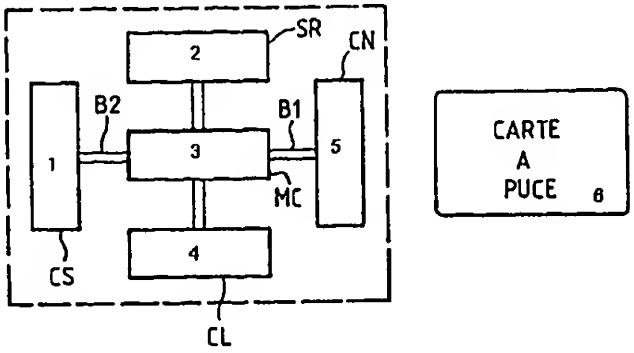
Avec rapport de recherche internationale.
Avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues.

(54) Title: SMART CARD READER WITH MICROCONTROLLER AND SECURITY COMPONENT

(54) Titre: LECTEUR DE CARTE A PUCE AVEC MICROCONTROLEUR ET COMPOSANT DE SECURITE

(57) Abstract

The invention concerns smart card readers dedicated to a particular application and using both a microcontroller (MC) whereof the read–only memory determines the operation of the application, and a security component (CS) executing, under the microcontroller control, sub–programmes related to the application security (authentication, confidential programmes and the like). In order that the application manager may access certain zones of the security component memory, it is provided that the microcontroller can automatically shift into a so–called "transparent" mode, when a specific access code transmitted by the test card is recognised. In this mode, the reading or writing instructions of a memory zone of the security component, transmitted by the test card, are interpreted by the microcontroller as being reading or writing instructions of a memory zone of the security component and not of the microcontroller. The invention is applicable to portable readers.



1...SECURITY COMPONENT
2...SCREEN
3...MICROCONTROLLER
4...KEYBOARD
5...SMART CARD INPUT CONNECTOR
6...SMART CARD

(57) Abrégé

L'invention concerne les lecteurs de carte à puce dédiés à une application particulière et utilisant à la fois un microcontrôleur (MC) dont la mémoire morte détermine le déroulement de l'application, et un composant de sécurité (CS) exécutant, sous le contrôle du microcontrôleur, des sous–programmes liés à la sécurité de l'application (authentification, programmes confidentiels, etc.). Pour que le gestionnaire de l'application puisse avoir accès à certaines zones de mémoire du composant de sécurité, on prévoit que le microcontrôleur peut passer automatiquement dans un mode dit "transparent", lors de la reconnaissance d'un code d'accès spécifique émis par une carte de test. Dans ce mode, les instructions de lecture ou écriture d'une zone de mémoire, émises par la carte de test, sont interprétées par le microcontrôleur comme étant des instructions de lecture ou écriture d'une zone de mémoire du composant de sécurité et non du microcontrôleur. Application aux lecteurs portables.

UNIQUEMENT A TITRE D'INFORMATION

Codes utilisés pour identifier les Etats parties au PCT, sur les pages de couverture des brochures publiant des demandes internationales en vertu du PCT.

AL	Albanie	ES	Espagne	LS	Lesotho	SI	Slovénie
AM	Arménie	FI	Finlande	LT	Lituanie	SK	Slovaquie
AT	Autriche	FR	France	LU	Luxembourg	SN	Sénégal
AU	Australie	GA	Gabon	LV	Lettonie	SZ	Swaziland
AZ	Azerbaïdjan	GB	Royaume-Uni	MC	Monaco	TD	Tchad
BA	Bosnie-Herzégovine	GE	Géorgie	MD	République de Moldova	TG	Togo
BB	Barbade	GH	Ghana	MG	Madagascar	TJ	Tadjikistan
BE	Belgique	GN	Guinée	MK	Ex-République yougoslave de Macédoine	TM	Turkménistan
BF	Burkina Faso	GR	Grèce			TR	Turquie
BG	Bulgarie	HU	Hongrie	ML	Mali	TT	Trinité-et-Tobago
BJ	Bénin	IE	Irlande	MN	Mongolie	UA	Ukraine
BR	Brésil	IL	Israël	MR	Mauritanie	UG	Ouganda
BY	Bélarus	IS	Islande	MW	Malawi	US	Etats-Unis d'Amérique
CA	Canada	IT	Italie	MX	Mexique	UZ	Ouzbékistan
CF	République centrafricaine	JP	Japon	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Pays-Bas	YU	Yougoslavie
CH	Suisse	KG	Kirghizistan	NO	Norvège	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	République populaire démocratique de Corée	NZ	Nouvelle-Zélande		
CM	Cameroun			PL	Pologne		
CN	Chine	KR	République de Corée	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Roumanie		
CZ	République tchèque	LC	Sainte-Lucie	RU	Fédération de Russie		
DE	Allemagne	LI	Liechtenstein	SD	Soudan		
DK	Danemark	LK	Sri Lanka	SE	Suède		
EE	Estonie	LR	Libéria	SG	Singapour		

LECTEUR DE CARTE A PUCE AVEC MICROCONTROLEUR ET COMPOSANT DE SECURITE

L'invention concerne les lecteurs de carte à puce, et plus particulièrement les lecteurs dont le fonctionnement est sécurisé par un composant de sécurité exécutant des programmes spécifiques liés à la sécurité d'une application.

On connaît des lecteurs de cartes à puces qui sont dédiés à l'exécution d'une application spécifique et qui doivent être sécurisés pour qu'il n'y ait pas de fraude lors de l'exécution de l'application (notamment lorsque l'application a des implications financières).

Ces lecteurs comportent un microcontrôleur pourvu d'une mémoire morte de programmes, pour exécuter un programme applicatif figé dans cette mémoire. Et ils comportent en outre un composant de sécurité, distinct du microcontrôleur, capable d'exécuter des programmes spécifiques (liés à la sécurité ou à des éléments confidentiels de l'application) sous la commande du microcontrôleur de telle manière que toute communication de données entre la carte à puce et le composant de sécurité passe obligatoirement par le microcontrôleur.

Le composant de sécurité est donc en quelque sorte lui aussi un microcontrôleur, avec ses mémoires de programmes, mais il n'est pas relié directement à un connecteur d'entrée du lecteur. Il ne communique qu'avec le microcontrôleur qui, lui, est relié au connecteur d'entrée. Le microcontrôleur peut donc communiquer soit avec la carte à puce insérée dans le connecteur d'entrée soit avec le composant de sécurité, et, étant donné que l'application est figée et se déroule dès l'introduction d'une carte à puce dans le

lecteur, c'est le microcontrôleur qui agit comme maître par rapport à la carte à puce et par rapport au composant de sécurité.

Pour illustrer le problème que vise à résoudre la présente invention, on peut donner l'exemple d'un lecteur de carte à puce dédié à une application particulière placée sous le contrôle d'un gestionnaire de l'application, et c'est ce gestionnaire qui vend des cartes à puces. Seules les cartes émises par le prestataire sont autorisées. Le composant de sécurité a notamment pour mission de détecter, à l'aide d'algorithmes de chiffrement et déchiffrement, que la carte placée dans le lecteur est une carte autorisée. Le microcontrôleur du lecteur pilote le déroulement de l'ensemble de l'application; il transmet des instructions au composant de sécurité et contrôle la communication de données entre la carte et le composant de sécurité.

L'utilisateur standard de l'application n'a évidemment pas accès aux programmes et aux données des mémoires non volatiles du composant de sécurité. Et le microcontrôleur programmé par une mémoire morte constitue la barrière nécessaire pour que cet utilisateur ne puisse ni savoir ce qui se passe dans le composant de sécurité, ni le modifier. Par exemple, si le programme nécessite que le composant de sécurité fournisse des données à la carte, il les fournit en principe sous forme cryptée. Et le programme de l'application, figé en mémoire morte ROM donc non modifiable par un utilisateur, ne prévoit pas d'accès aux zones de mémoire non volatile du composant de sécurité.

Mais le gestionnaire de l'application peut avoir besoin, pour des raisons de test, de diagnostic de

défauts, ou même de nécessité de légères modifications dans les paramètres de l'application, de contrôler certains contenus de mémoire du composant de sécurité, ou de modifier ces contenus.

Une solution serait de laisser en partie accessibles les bornes du composant de sécurité, par exemple pour qu'on puisse y accéder par l'intermédiaire de pointes de test après ouverture du lecteur. Mais en pratique, pour des raisons de sécurité, on préfère noyer complètement dans une résine les broches d'accès du composant de sécurité.

On pourrait aussi envisager que la mémoire morte de programme du microcontrôleur contienne, outre le programme de l'application à laquelle le lecteur est dédié, d'autres programmes déclenchés par des protocoles spéciaux. Ces programmes seraient donc présents par avance dans la mémoire morte du microcontrôleur et comprendraient a priori tous les programmes d'accès en lecture ou en écriture que le gestionnaire de l'application pourrait avoir besoin d'utiliser ultérieurement. C'est difficilement envisageable, et même dangereux si les données secrètes doivent être utilisées (code secret par exemple).

La présente invention a pour but de proposer un moyen pour que le gestionnaire de l'application puisse accéder facilement, à des fins de test, de diagnostic, ou de modification, au composant de sécurité, c'est-à-dire en pratique à certaines zones de mémoire de ce composant de sécurité, et ceci sans mettre en péril la sécurité de l'application.

Pour cela, l'invention propose un lecteur de carte à puce dont le microcontrôleur possède deux modes de fonctionnement qui sont un fonctionnement normal, à usage d'un utilisateur standard, pour l'exécution du

programme applicatif figé auquel le lecteur est dédié, et un fonctionnement "transparent", dont l'utilisateur standard n'a pas l'usage, dans lequel le microcontrôleur peut recevoir d'une carte à puce ou d'une sonde simulant une carte à puce, des instructions d'accès qu'il interprète non pas comme des instructions d'accès à ses propres mémoires, mais comme des instructions d'accès aux mémoires du composant de sécurité.

Plus précisément, l'invention propose un lecteur de carte comportant un connecteur d'entrée, un microcontrôleur, et un composant de sécurité exécutant des programmes sous la commande du microcontrôleur, le microcontrôleur possédant un mode de fonctionnement normal dans lequel il exécute un programme contenu dans sa mémoire morte, caractérisé en ce que le microcontrôleur possède également un mode de fonctionnement dit "transparent", dans lequel il se place automatiquement à réception d'un code spécifique sur le connecteur d'entrée, et dans lequel il reçoit du connecteur d'entrée des instructions d'adressage de zones de mémoire et il exécute ces instructions en les interprétant comme étant des ordres d'accès à des zones de mémoire du composant de sécurité.

Ainsi, bien que le composant de sécurité ne puisse pas être en communication directe avec le connecteur d'entrée, il devient possible d'accéder à des zones de mémoire de ce composant : après passage dans le mode transparent, une adresse d'accès à une zone de mémoire cesse d'être interprétée comme une adresse de mémoire du microcontrôleur et devient une adresse de mémoire du composant de sécurité. Le microcontrôleur exécutera alors un sous-programme d'adressage du composant de sécurité. Inversement, dans le mode normal, une

instruction d'adressage de zone de mémoire fournie par le connecteur d'entrée est toujours interprétée comme étant une instruction d'adressage d'une zone de mémoire du microcontrôleur.

En pratique, le mode de fonctionnement transparent comporte quatre instructions principales qui sont respectivement :

- mise sous tension du composant de sécurité;
- lecture d'une donnée à une adresse de mémoire;
- écriture d'une donnée à une adresse de mémoire;
- mise hors tension du composant de sécurité.

Si le composant de sécurité possède une mémoire non volatile électriquement programmable, notamment pour des raisons de personnalisation, il sera possible d'accéder à cette mémoire, pour le gestionnaire de l'application mais pas pour l'utilisateur standard, pour en changer les données. Le mode de fonctionnement transparent permettra donc de modifier le contenu de zones qui ne sont pas modifiables par le programme exécuté en mode normal.

D'autres caractéristiques et avantages de l'invention apparaîtront à la lecture de la description détaillée qui suit et qui est faite en référence aux dessins annexés dans lesquels :

- la figure 1 représente la configuration générale d'un lecteur de carte à puce à microcontrôleur et à composant de sécurité;
- la figure 2 représente la constitution interne du microcontrôleur;
- la figure 3 représente la constitution interne du composant de sécurité;

- la figure 4 représente un tableau des séquences exécutées par le microcontrôleur et la carte de test pour aboutir au passage en mode transparent;

- les figures 5 à 8 représentent des diagrammes de séquences exécutées par le microcontrôleur, le composant de sécurité et la carte (de test) lors de l'exécution de chacune des instructions principales du mode transparent.

Le lecteur comporte un connecteur de carte à puce CN, un microcontrôleur MC et un composant de sécurité CS. Selon l'application auquel le lecteur est dédié, il peut comprendre aussi une interface homme-machine, par exemple un clavier CL et un écran SR, pour permettre à l'utilisateur d'entrer ou de lire des données si c'est nécessaire pour l'application. Le déroulement de l'application sera en général déclenché simplement par l'introduction d'une carte à puce dans le lecteur. Il peut y avoir plusieurs applications et une sélection d'une application peut être effectuée par exemple par le clavier. Mais de toutes façons, il s'agit d'applications figées dans une mémoire morte non modifiable.

Le connecteur de carte CN constitue l'entrée du lecteur (en général une entrée à six ou huit contacts, l'échange de données s'effectuant par une communication de type série sur l'un des contacts).

Le microcontrôleur MC est relié au connecteur d'entrée CN par un premier bus de liaison B1; il est relié au composant de sécurité CS par un deuxième bus de liaison B2. Il n'y a pas de liaison directe permettant le passage de données entre le composant de sécurité et le connecteur d'entrée.

Le composant de sécurité est soudé sur un circuit imprimé formant le coeur du lecteur, à l'intérieur de ce dernier. Ses broches de connexion ne sont pas physiquement accessibles (en général même pas par des pointes de test car les broches sont recouvertes d'une résine de protection).

Cette impossibilité d'accès au composant de sécurité est volontaire; pour l'utilisation standard de la carte, seuls les accès prévus à l'avance dans le programme d'application figé du microcontrôleur sont autorisés et sont effectués par l'intermédiaire du microcontrôleur.

Le microcontrôleur, dans ce type de lecteur dédié à une application bien précise, possède de la mémoire de programme de type ROM, c'est-à-dire une mémoire non modifiable (mémoire morte) qui contient les séquences d'instruction permettant le déroulement de l'application. Le microcontrôleur possède également de la mémoire RAM permettant le stockage temporaire de données volatiles. Ces mémoires sont associées à un microprocesseur MP1 qui forme le coeur de l'intelligence du microcontrôleur. Enfin il possède des lignes d'entrée/sortie en nombre suffisant pour communiquer avec les composant de sécurité CS d'une part, avec le connecteur d'entrée CN d'autre part, et éventuellement avec le clavier CL et l'écran SR. La figure 2 représente la structure du microcontrôleur.

Le composant de sécurité a une structure similaire (figure 3) car il est en pratique constitué par un microcontrôleur (c'est-à-dire un microprocesseur MP2 pourvu de mémoires de programmes et de travail), mais, comme indiqué ci-dessus, il ne communique qu'avec le microcontrôleur et non avec la carte à puce. Il est capable d'exécuter des programmes placés dans sa

mémoire morte ROM. En outre, il possède de préférence une partie de mémoire non volatile, inscriptible et effaçable électriquement (mémoire EEPROM). Dans cette mémoire électriquement programmable, on peut placer des données de personnalisation des programmes exécutés par le composant de sécurité. On peut placer aussi des données représentant des paramètres variables de ces programmes.

Le composant de sécurité est capable de recevoir sur ses lignes d'entrée des ordres et des données. Il exécute les ordres, enregistre en mémoire les données, et renvoie sur ses lignes de sortie des résultats d'ordres qu'il a exécutés, notamment des résultats de calcul secrets effectués par les programmes qu'il possède dans ses mémoires non volatiles (ROM et EEPROM).

La carte à puce qu'on introduit dans le lecteur est capable de fournir des commandes et des données au microcontrôleur, et plus généralement de communiquer avec le microcontrôleur. Dans l'utilisation standard du lecteur, l'utilisateur possède une carte à puce qu'il introduit dans le lecteur pour lancer l'application. Mais on peut également, pour la mise en oeuvre de l'invention, introduire dans le lecteur une sonde, c'est-à-dire une carte simulée, ayant les contacts requis pour communiquer avec les entrées du lecteur, mais reliée par ailleurs à un terminal d'ordinateur. Cette carte simulée permet une communication entre l'extérieur et le lecteur pour des opérations de test ou de mise au point. Des cartes à puces de test non reliées à un ordinateur, mais capables de commander le déroulement de programmes de test et de recueillir des données de test, pourraient aussi être prévues pour les

besoins du gestionnaire de l'application (mais pas pour les utilisateurs standards du lecteur).

Le composant de sécurité CS et la carte à puce sont tous deux des périphériques esclaves du microcontrôleur MC dans l'application exécutée, en ce sens que c'est le microcontrôleur qui exécute le programme de l'application, la carte à puce et le composant de sécurité exécutant des ordres lorsqu'ils sont sollicités par le microcontrôleur dans le déroulement du programme. La carte et le composant de sécurité reçoivent donc des commandes (lecture, écriture, exécution de programmes contenus dans la carte ou le composant de sécurité), les exécutent, et renvoient les résultats d'exécution au microcontrôleur.

Le microcontrôleur est donc maître en ce qui concerne la communication avec une carte à puce standard et la communication avec le composant de sécurité.

Les utilisateurs du lecteur, qu'on appellera utilisateurs standard, ne peuvent faire qu'une seule chose : lancer l'exécution du programme applicatif standard contenu dans la mémoire ROM du microcontrôleur.

Pour bien faire comprendre le fonctionnement des trois composants (carte à puce, microcontrôleur, composant de sécurité) dans le déroulement de l'application standard, on se réfère à nouveau à une application de jeu de hasard, avant de décrire plus précisément l'invention.

L'utilisateur standard possède une carte à puce qui a été émise par le gestionnaire de l'application. Cette carte possède des éléments permettant de l'authentifier, sous forme de données enregistrées en mémoire (données pouvant être vérifiées par le

composant de sécurité) et éventuellement sous forme de programmes d'authentification qui, par comparaison avec des programmes contenus dans le composant de sécurité, permettront une authentification de la carte par ce dernier.

L'utilisateur introduit sa carte dans le lecteur. Selon la norme ISO 7816-3, le microcontrôleur du lecteur détecte l'introduction de la carte, la met alors sous tension, et lui envoie sa première commande "RESET".

La carte reçoit cette commande et envoie une "REPONSE AU RESET"; cette réponse permet une reconnaissance du type de carte de manière que la communication puisse être poursuivie selon un protocole déterminé.

Les procédures d'authentification de la carte se déroulent alors entre la carte et le composant de sécurité, sous le contrôle du microcontrôleur qui reste maître.

Par exemple, le microcontrôleur met le composant de sécurité sous tension, reçoit sa réponse au reset, puis lui demande un nombre aléatoire, reçoit ce nombre et le retransmet à la carte. Celle-ci code ce nombre aléatoire à l'aide d'un programme de chiffrement qu'elle possède. Elle renvoie au composant de sécurité, par l'intermédiaire du microcontrôleur, le nombre crypté, une donnée et une signature. Le composant de sécurité vérifie l'authenticité, notamment en vérifiant que la valeur cryptée est la bonne, en vérifiant la concordance de la donnée et de la signature, ou éventuellement par d'autres moyens.

Si l'authenticité est acquise, l'utilisateur peut demander de transférer la donnée dans le composant de sécurité. Si l'utilisateur doit entrer la donnée à

transférer, il faut bien sûr que le lecteur comporte des périphériques (clavier, écran) permettant de faire une sélection; ces périphériques sont gérés eux aussi par le microcontrôleur et son programme.

Le composant de sécurité calcule la nouvelle donnée de la carte et une nouvelle signature de la carte. Donnée et signature sont cryptés et transmis au microcontrôleur qui les inscrit dans la carte à puce en vue d'un échange futur.

Dès lors, l'application peut démarrer.

L'application est exécutée par un programme contenu dans la mémoire non volatile (ROM et EEPROM) du composant de sécurité.

Ce qui se passe dans le composant de sécurité, et notamment ce qui est contenu dans les mémoires non volatiles du composant de sécurité reste parfaitement inconnu de l'utilisateur standard et non modifiable. Il n'y a pas d'accès à volonté aux mémoires du composant de sécurité.

Mais le gestionnaire de l'application peut au contraire souhaiter avoir accès à l'intérieur du composant de sécurité pour des opérations de test, de diagnostic de défauts, ou même de modification des données de l'application.

L'invention résout ce problème en prévoyant le passage automatique du microcontrôleur dans un mode de fonctionnement "transparent", différent du mode de fonctionnement normal, lorsqu'une carte spéciale (ou une sonde simulant une carte et reliée à un ordinateur) est introduite dans le lecteur. Ce passage en mode transparent n'est pas autorisé pour les utilisateurs standards, et il résulte automatiquement de la reconnaissance d'un code spécifique à l'entrée du lecteur lors de l'introduction de la carte spéciale.

En pratique, le passage dans le mode transparent se déroule de la manière suivante : le gestionnaire de l'application, qui possède la carte à puce spéciale ou la sonde comportant le code spécifique, peut l'introduire dans le connecteur du lecteur. L'insertion de cette carte ou sonde est détectée par le lecteur selon une procédure classique (un simple contact sert à la détection). Cette détection provoque de la part du microcontrôleur une mise sous tension de la carte avec commande de réinitialisation (RESET). La commande de réinitialisation implique une réponse de la carte (Réponse au reset). La réponse au reset comprend d'abord (selon la norme ISO 7816-3) des informations sur le protocole de communication qui sera utilisé par la suite, puis un champ de données que la norme laisse libre. Un code spécifique, non connu des utilisateurs standards de la carte à puce est placé par la carte spéciale dans ce champ. La réponse au reset de la carte spéciale inclut donc ce code spécifique.

Le code spécifique est reconnu par le microcontrôleur et déclenche le passage en mode "transparent".

Dans le mode transparent, des commandes de lecture ou d'écriture en mémoire, en provenance de l'entrée du lecteur, c'est-à-dire en provenance de la carte spéciale ou la sonde, peuvent être reçues par le microcontrôleur. Ces ordres sont accompagnés de l'adresse de mémoire qu'il faut lire ou écrire. Mais le microcontrôleur interprète alors ces adresses comme étant des adresses de lecture ou d'écriture dans une mémoire du composant de sécurité et non comme une adresse de lecture ou d'écriture dans une mémoire du microcontrôleur comme il le ferait dans le mode de fonctionnement normal.

Le passage en mode transparent peut consister dans l'initialisation d'un bit d'état ou drapeau dans un registre du microcontrôleur, ce drapeau restant dans un état par défaut correspondant au mode normal tant que le code spécifique n'a pas été reconnu par le microcontrôleur et revenant dans cet état par défaut lors du retour au mode normal. Le retour au mode normal est effectué par une instruction spécifique donnée à partir de la carte, ou à la suite d'un incident (retrait de la carte hors du lecteur, etc.).

Ce bit d'état déroute alors les commandes de lecture ou d'écriture reçues par le microcontrôleur en provenance de la carte, et les aiguille vers des sous-programmes (en mémoire morte du microcontrôleur) contenant simplement un ordre de lecture ou d'écriture adressé au composant de sécurité. Les paramètres affectés à cet ordre, c'est-à-dire l'adresse où il faut lire ou écrire avec la donnée à écrire, sont ceux qui sont reçus de la carte à puce et ils sont transmis tels quels par le sous-programme. On comprendra que ces sous-programmes en mémoire morte du microcontrôleur ne comprennent que l'instruction de lecture ou écriture adressée au composant de sécurité, mais ne comprennent ni l'adresse à laquelle il faut lire ou écrire ni la donnée à écrire. L'adresse et les données sont simplement transportées de la mémoire de travail du microcontrôleur vers le composant de sécurité. C'est ce qui permet d'avoir un accès à n'importe quelle adresse de mémoire du composant de sécurité sans encombrer la mémoire morte du microcontrôleur de toutes les adresses auxquelles on peut vouloir lire ou écrire dans le composant de sécurité lors des programmes de test ou de mise au point.

En cas de lecture dans une zone de mémoire du composant de sécurité, le composant de sécurité transmet la donnée lue au microcontrôleur qui la retransmet à la carte à puce.

Outre les commandes de lecture et d'écriture, le mode transparent peut comporter un petit nombre de commandes en provenance de la carte à puce, et notamment :

- un ordre de mise sous tension du composant de sécurité, entraînant une réponse au reset de ce dernier et une écriture de la réponse dans la carte;
- un ordre de mise hors tension du composant de sécurité, entraînant également le retour du microcontrôleur dans son mode normal;
- éventuellement un ordre bidirectionnel comprenant une écriture de données et une lecture de données dans le composant de sécurité.

Un code d'instruction peut être affecté à chacune des commandes possibles; le code d'instruction correspondant à la lecture ou à l'écriture peut être exactement le même code qui servirait à la lecture ou à l'écriture en mode normal mais il se traduit par une exécution différente dans le mode transparent puisqu'il va alors consister en une lecture ou une écriture dans le composant de sécurité et non dans les mémoires du microcontrôleur.

D'une manière générale, dans le mode de fonctionnement transparent, on peut prévoir que le microcontrôleur reste maître tout en exécutant des instructions fournies par la carte spéciale, et ceci de la manière suivante : c'est le microcontrôleur qui envoie systématiquement à la carte, lorsqu'il a fini l'exécution d'une séquence précédente, une commande de lecture de la carte. Autrement dit, il se met en

permanence à l'écoute d'une commande possible en provenance de la carte.

Pour rester compatible avec les protocoles de la norme ISO 7816-3, on peut prévoir par exemple que dans le mode de fonctionnement transparent le microcontrôleur envoie systématiquement une commande de lecture de la carte; celle-ci renvoie d'abord la longueur de la commande qui va suivre; le microcontrôleur envoie ensuite à la carte une demande de résultat (le résultat est la commande proprement dite). La carte envoie la commande et un mot d'état. Le microcontrôleur vérifie le mot d'état et exécute la commande (c'est-à-dire qu'en pratique, dans le mode transparent, il la fait exécuter par le composant de sécurité); puis il renvoie un résultat s'il y a lieu; la carte envoie un acquittement. Le microcontrôleur peut renvoyer une commande de lecture.

Les diagrammes des figures 4 à 8 résument les séquences exécutées par le microcontrôleur, le composant de sécurité, et la carte spéciale pour diverses instructions exécutées en mode transparent.

Le diagramme de la figure 4 correspond aux séquences de passage en mode transparent; les séquences exécutées sont les suivantes :

- par le microcontrôleur : détection de la présence d'une carte, mise sous tension (reset) de la carte, attente de réponse au reset;
- par la carte : réponse au reset avec code spécifique dans la réponse;
- par le microcontrôleur : analyse de la réponse au reset; reconnaissance du code spécifique; passage au mode transparent, avec établissement du drapeau de signalisation du mode transparent.
- par le composant de sécurité : pas d'action.

La figure 5 correspond à une commande de mise sous tension du composant de sécurité :

- par le microcontrôleur : envoi d'une commande de lecture à la carte; attente de la réponse;
- par la carte : réception; envoi de la longueur de la commande qui va suivre;
- par le microcontrôleur : réception de la réponse de la carte; envoi d'une demande de résultat; attente de la réponse;
- par la carte : réception du message; envoi d'une commande de mise sous tension du composant de sécurité;
- par le microcontrôleur : réception de la réponse de la carte; mise sous tension et reset du composant de sécurité; attente de la réponse au reset;
- par le composant de sécurité : envoi de la réponse au reset;
- par le microcontrôleur : réception de la réponse, envoi d'un ordre d'écriture de la réponse dans la carte; attente d'un acquittement de la part de la carte;
- par la carte : exécution de l'ordre d'écriture; envoi de l'acquittement.

La figure 6 correspond à un envoi d'ordre sortant vers le composant de sécurité (lecture de données) :

- par le microcontrôleur : envoi d'une commande de lecture à la carte; attente de la réponse;
- par la carte : réception; envoi de la longueur de la commande qui va suivre;
- par le microcontrôleur : réception de la réponse de la carte; envoi d'une demande de résultat; attente de la réponse;

- par la carte : réception du message; envoi d'une commande de lecture, avec adresse de zone de mémoire du composant de sécurité;

- par le microcontrôleur : réception de la réponse de la carte; interprétation de la commande; envoi d'une commande de lecture du composant de sécurité, à l'adresse indiquée par la carte; attente de la réponse du composant de sécurité;

- par le composant de sécurité : réception du message, exécution, envoi de la réponse;

- par le microcontrôleur : réception de la réponse, envoi d'un ordre d'écriture de la réponse dans la carte; attente d'un acquittement de la part de la carte;

- par la carte : réception du message; exécution de l'ordre d'écriture; envoi de l'acquittement.

La figure 7 correspond à l'envoi d'un ordre entrant (écriture dans une mémoire du composant de sécurité). Cet ordre est particulièrement important pour écrire dans une mémoire non-volatile (EEPROM) du composant de sécurité, par exemple pour modifier la personnalisation du lecteur ou pour modifier des paramètres de l'application :

- par le microcontrôleur : envoi d'une commande de lecture à la carte; attente de la réponse;

- par la carte : réception; envoi de la longueur de la commande qui va suivre;

- par le microcontrôleur : réception de la réponse de la carte; envoi d'une demande de résultat; attente de la réponse;

- par la carte : réception du message; envoi d'une commande d'écriture dans le composant de sécurité, avec adresse d'écriture et donnée à écrire;

- par le microcontrôleur : réception de la réponse de la carte; interprétation de la commande; envoi d'une commande d'écriture dans le composant de sécurité, avec la donnée indiquée par la carte et l'adresse indiquée par la carte;

- par le composant de sécurité : réception du message; exécution de la commande d'écriture; envoi d'un mot d'état représentant l'état d'exécution de la commande;

- par le microcontrôleur : réception du message, envoi d'un ordre d'écriture du mot d'état dans la carte; attente d'un acquittement de la part de la carte;

- par la carte : exécution de l'ordre d'écriture; envoi de l'acquittement.

Pour un ordre bidirectionnel (écriture + lecture) le principe serait le même.

La figure 8 correspond à la mise hors tension du composant de sécurité et à la sortie du mode transparent :

- par le microcontrôleur : envoi d'une commande de lecture à la carte; attente de la réponse;

- par la carte : réception; envoi de la longueur de la commande qui va suivre;

- par le microcontrôleur : réception de la réponse de la carte; envoi d'une demande de résultat; attente de la réponse;

- par la carte : réception du message; envoi d'une commande de mise hors tension du composant de sécurité, avec un mot d'état de la carte;

- par le microcontrôleur : réception de la réponse de la carte; vérification du mot d'état; mise hors tension du composant de sécurité; rétablissement du

drapeau de mode transparent à sa valeur par défaut correspondant au mode normal.

REVENDICATIONS

1. Lecteur de carte à puce comportant un connecteur d'entrée (CN), un microcontrôleur (MC), et un composant de sécurité (CS) exécutant des programmes sous la commande du microcontrôleur, le microcontrôleur possédant un mode de fonctionnement normal dans lequel il exécute un programme contenu dans sa mémoire morte, caractérisé en ce que le microcontrôleur possède également un mode de fonctionnement dit "transparent", dans lequel il se place automatiquement à réception d'un code spécifique sur le connecteur d'entrée, et dans lequel il reçoit du connecteur d'entrée des instructions d'adressage de zones de mémoire et il exécute ces instructions en les interprétant comme étant des ordres d'accès à des zones de mémoire du composant de sécurité.

2. Lecteur de carte selon la revendication 1, caractérisé en ce que le composant de sécurité ne peut communiquer avec le connecteur d'entrée que par l'intermédiaire du microcontrôleur et sous la commande de celui-ci.

3. Lecteur de carte selon l'une des revendications 1 et 2, caractérisé en ce que le lecteur est dédié à une application déterminée dont l'exécution est définie par le programme contenu dans la mémoire morte du microcontrôleur, cette application ne comportant pas de possibilité d'accès à certaines zones de mémoire du composant de sécurité.

4. Lecteur de carte selon l'une des revendications précédentes, caractérisé en ce que le mode de fonctionnement transparent comporte quatre instructions principales qui sont respectivement :

- mise sous tension du composant de sécurité;
- lecture d'une donnée à une adresse de mémoire;
- écriture d'une donnée à une adresse de mémoire;
- mise hors tension du composant de sécurité.

5. Lecteur de carte selon l'une des revendications précédentes, caractérisé en ce que le composant de sécurité possède une mémoire électriquement programmable, et en ce que le mode de fonctionnement transparent permet l'accès à cette mémoire pour modifier le contenu de zones qui ne sont pas modifiables par le programme exécuté en mode normal.

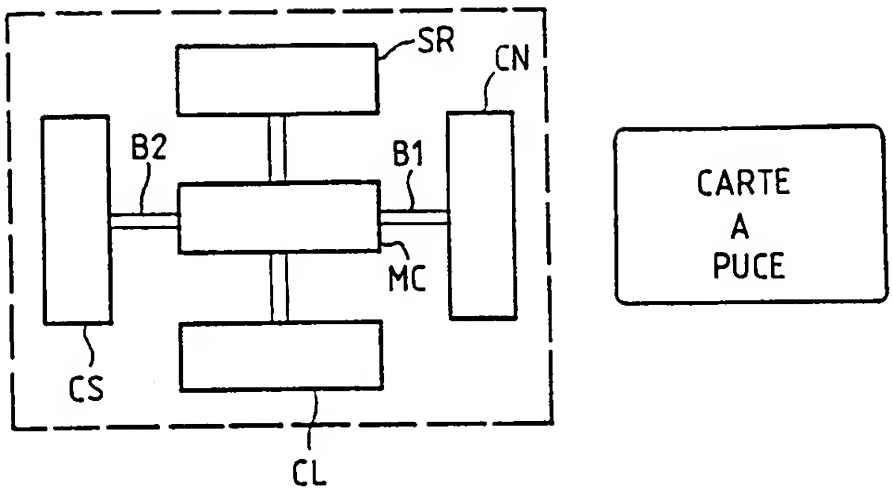


FIG_1

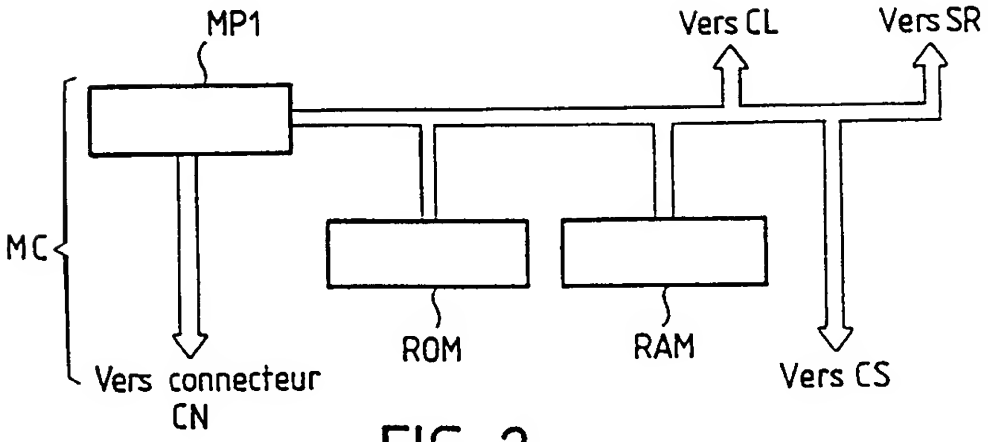


FIG_2

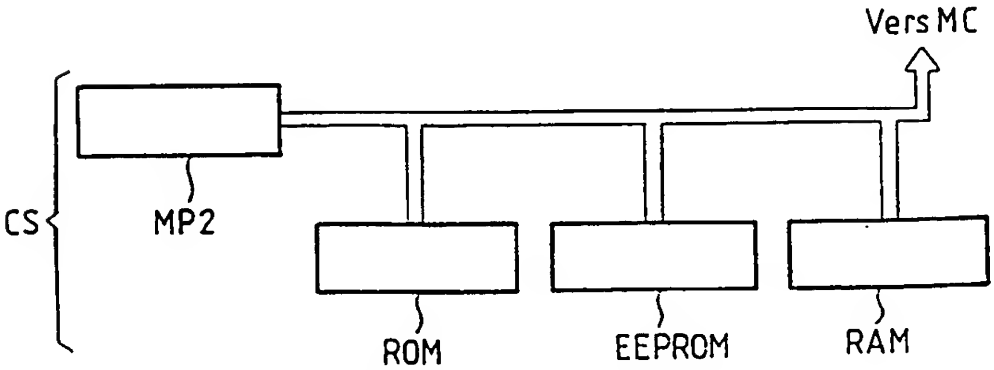


FIG_3

PASSAGE AU MODE TRANSPARENT

Composant de sécurité	Microcontrôleur	Carte à puce
	1. Détection présence de carte	
	2. reset carte	
	3. Attente réponse	
		4. réponse au reset avec code spécifique
	5. réception message	
	6. établissement d'un drapeau de mode transparent	

FIG. 4

MISE SOUS TENSION DE CS

Composant de sécurité	Microcontrôleur	Carte à puce
	1. Envoi commande de lecture	
		2. réception message
		3. envoi longueur de commande
	4. réception message	
	5. envoi demande de résultat	
		6. réception message
		7. envoi commande de mise sous tension
	8. réception message	
	9. mise sous tension et reset de CS	
10. réponse au reset		
	11. réception message	
	12. envoi ordre d'écriture de la réponse dans la carte	
	13. attente acquittement	
		14. réception message
		15. exécution de l'écriture
		15. envoi acquittement
	17. réception acquittement	

FIG. 5

ORDRE DE LECTURE

Composant de sécurité	Microcontrôleur	Carte à puce
	1. Envoi commande de lecture	
		2. réception message
		3. envoi longueur de commande
	4. réception message	
	5. envoi demande de résultat	
		6. réception message
		7. envoi commande de lecture, avec adresse AD
	8. réception message	
	9. interprétation = envoi commande de lecture à CS avec adresse AD	
10. réception message		
11. exécution		
12. envoi des données		
	13. réception message	
	14. envoi commande d'écriture de la réponse dans la carte	
	15. attente acquittement	
		16. réception message
		17. exécution écriture
		18. envoi acquittement
	19. réception acquittement	

FIG. 6

ORDRE D'ECRITURE

Composant de sécurité	Microcontrôleur	Carte à puce
	1. Envoi commande de lecture	
		2. réception message
		3. envoi longueur de commande
	4. réception message	
	5. envoi demande de résultat	
		6. réception message
		7. envoi commande d'écriture, avec adresse AD et donnée DT à écrire
	8. réception message	
	9. interprétation = envoi commande d'écvriture à CS avec adresse AD et donnée DT	
10. réception message		
11. exécution		
12. envoi mot d'état		
	13. réception message	
	14. envoi commande d'écriture du mot d'état dans la carte	
	15. attente acquittement	
		16. réception message
		17. exécution écriture
		18. envoi acquittement
	19. réception acquittement	

FIG. 7

MISE HORS TENSION DE CS
ET RETOUR AU MODE NORMAL

Composant de sécurité	Microcontrôleur	Carte à puce
	1. Envoi commande de lecture	
		2. réception message
		3. envoi longueur de commande
	4. réception message	
	5. envoi demande de résultat	
		6. réception message
		7. envoi commande de mise hors tension de CS
	8. réception message	
	9. mise hors tension de CS	
	10. retour du drapeau à sa valeur de mode normal	

FIG. 8

INTERNATIONAL SEARCH REPORT

Int. ional Application No
PCT/FR 98/01659

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G07F7/10

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G07F G06K

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	EP 0 707 290 A (CP8 TRANSAC) 17 April 1996 see abstract; claims; figures see column 5, line 16 - column 6, line 42	1-5
Y	DE 34 35 697 A (ROBERT BOSCH) 3 April 1986 see the whole document	1-5
A	US 5 390 331 A (TAKAAKI YUI) 14 February 1995	

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
8 December 1998	17/12/1998

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	David, J

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inter nal Application No
PCT/FR 98/01659

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0707290 A	17-04-1996	FR 2725537 A	12-04-1996
		AU 690324 B	23-04-1998
		AU 3318795 A	16-05-1996
		BR 9504355 A	08-10-1996
		CA 2160223 A	12-04-1996
		JP 8212066 A	20-08-1996
		NO 954028 A	12-04-1996
		US 5825875 A	20-10-1998
DE 3435697 A	03-04-1986	NONE	
US 5390331 A	14-02-1995	JP 3022026 A	30-01-1991

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/FR 98/01659

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 6 G07F7/10

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 6 G07F G06K

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
Y	EP 0 707 290 A (CP8 TRANSAC) 17 avril 1996 voir abrégé; revendications; figures voir colonne 5, ligne 16 - colonne 6, ligne 42	1-5
Y	DE 34 35 697 A (ROBERT BOSCH) 3 avril 1986 voir le document en entier	1-5
A	US 5 390 331 A (TAKAAKI YUI) 14 février 1995	

☐ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
8 décembre 1998	17/12/1998

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	David, J

1

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Der a internationale No
PCT/FR 98/01659

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
EP 0707290 A	17-04-1996	FR 2725537 A	12-04-1996
		AU 690324 B	23-04-1998
		AU 3318795 A	16-05-1996
		BR 9504355 A	08-10-1996
		CA 2160223 A	12-04-1996
		JP 8212066 A	20-08-1996
		NO 954028 A	12-04-1996
		US 5825875 A	20-10-1998
DE 3435697 A	03-04-1986	AUCUN	
US 5390331 A	14-02-1995	JP 3022026 A	30-01-1991